EP 26744 @

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 176 826 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
30.01.2002 Bulletin 2002/05

(51) Int Cl.[7]: **H04N 7/167**

(21) Application number: **01117554.4**

(22) Date of filing: **20.07.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **21.07.2000 US 621476**

(71) Applicant: **Hughes Electronics Corporation**
El Segundo, California 90245-0956 (US)

(72) Inventors:
- **Kahn, Raynold M.**
  Los Angeles, California 90036 (US)
- **Gagnon, Gregory J.**
  Torrance, California 90277 (US)
- **Ha, David D.**
  San Gabriel, California 91755 (US)
- **Klauss, Peter M.**
  Torrance, California 90503 (US)
- **Curren, Christopher P.**
  Brentwood, California 90049 (US)
- **James, Thomas H.**
  Pacific Palisades, California 90272 (US)

(74) Representative:
Grünecker, Kinkeldey, Stockmair & Schwanhäusser Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

(54) Super encrypted storage and retrieval of media programs in a hard-paired receiver and storage device

(57) A method and apparatus for storing and retrieving program material for subsequent replay is disclosed. The apparatus comprises a tuner (410), for receiving a data stream comprising encrypted access control information and the program material encrypted according to a first (CW) encryption key, the access control information including the first encryption key; a first encryption module (552), communicatively coupled to the tuner (410) and communicatively coupleable to a media storage device (524), for further encrypting the encrypted program material according to a second encryption key (514) and for encrypting the second encryption key (514) according to a third encryption key (518) to produce a fourth encryption key (520); a first decryption module (550) communicatively coupleable to the media storage device (524), for decrypting the fourth encryption key (520) retrieved from the media storage device (524) using the third encryption key (518) to produce the second encryption key (514), and for decrypting the further encrypted program material (510) retrieved from the media program device (524) to produce the encrypted program material (514); a conditional access module (406) communicatively coupled to the first decryption module (552), for decrypting the encrypted access control information to produce the first (CW) encryption key; and a second decryption module (540), for decrypting the program material using the first (CW) encryption key.

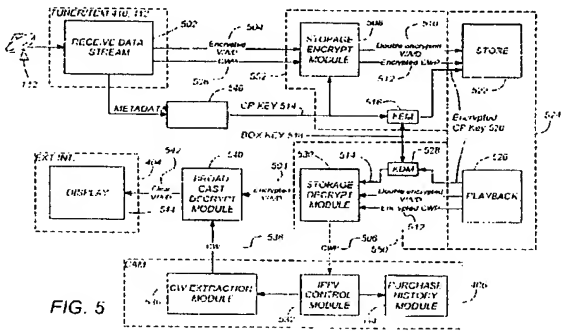

FIG. 5

EP 1 176 826 A2

Description

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is related to the following patent applications, all of which applications are hereby incorporated by reference herein:

U.S. Patent Application Serial No. --/---,---, entitled "SECURE STORAGE AND REPLAY OF MEDIA PROGRAMS USING A HARD-PAIRED RECEIVER AND STORAGE DEVICE," by Raynold M. Kahn, Gregory J. Gagnon, David D. Ha, Peter M. Klauss, Christopher P. Curren, and Thomas H. James, attorney's docket number PD-200042, filed on same date herewith;

U.S. Patent Application Serial No. --/---,---, entitled "SUPER ENCRYPTED STORAGE AND RETRIEVAL OF MEDIA PROGRAMS WITH MODIFIED CONDITIONAL ACCESS FUNCTIONALITY, " by Raynold M. Kahn, Gregory J. Gagnon, David D. Ha, Peter M. Klauss, Christopher P. Curren, and Thomas H. James, attorney's docket number PD-200044, filed on same date herewith;

U.S. Patent Application Serial No. --/---,---, entitled "SUPER ENCRYPTED STORAGE AND RETRIEVAL OF MEDIA PROGRAMS WITH SMARTCARD GENERATED KEYS," by Raynold M. Kahn, Gregory J. Gagnon, David D. Ha, Peter M. Klauss, Christopher P. Curren, and Thomas H. James, attorney's docket number PD-200045, filed on same date herewith;

U.S. Patent Application Serial No. --/---,---, entitled "VIDEO ON DEMAND PAY PER VIEW SERVICES WITH UNMODIFIED CONDITIONAL ACCESS FUNCTIONALITY" by Raynold M. Kahn, Gregory J. Gagnon, David D. Ha, Peter M. Klauss, Christopher P. Curren, and Thomas H. James, attorney's docket number PD-200055, filed on same date herewith; and

U.S. Patent Application Serial No. 09/491,959, entitled "VIRTUAL VIDEO ON DEMAND USING MULTIPLE ENCRYPTED VIDEO SEGMENTS," by Robert G. Arsenault and Leon J. Stanger, attorney's docket number PD-980208, filed on January 26, 2000.

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0002] The present invention relates to systems and methods for providing video program material to subscribers, and in particular to a method and system for securely storing and replaying media programs.

2. Description of the Related Art

[0003] In recent years, there has been increasing interest in allowing cable and satellite television subscribers to record broadcast media programs for later viewing. This capability, hereinafter referred to as personal video recording (PVR), can be used to provide video-on-demand (VOD) services, or simply to allow the subscriber to save media programs for repeated viewing and/or archival purposes.

[0004] In the past, video cassette tape recorders (VCRs) have been used for such personal video recording. Recently, however, hard disks, similar to those used in personal computers, have been used to store media programs for later viewing. Unlike VCRs, such devices typically do not include a tuner, and are instead coupled to the satellite receiver or cable box. Also unlike VCRs, these devices are typically used to record digital content, not analog video. This difference is both advantageous and disadvantageous.

[0005] An advantage of such devices is that they permit long term storage and multiple replays without substantial degradation. Another advantage is that they permit more rapid trick-play functions such as fast forwarding and rewinding. A disadvantage of such devices is that they are capable of making multiple-generation copies of the program material as well, and without serious degradation. This raises the very real possibility that the multiple generation copies of the media programs will be produced and distributed without permission. This possibility has caused some media providers to be reluctant to allow their media programs to be recorded by such devices.

[0006] To ameliorate this problem, it is critical to protect the stored media programs with strong security and copy control. Current devices do not scramble media programs before storage, nor do they store copy protection information. Instead, such devices record decrypted program content into the storage disk using a paired hardware scheme in which the hard disk controller and hard disk are paired to each other specifically through a specific interface. Because the hard disk controller and the disk itself are essentially paired together, storage or playback will not function if the disk were to be removed and transferred to another player. The weakness of this security scheme is that it relies only on the paired hardware to ensure security ... the media programs stored on the disk drive itself are not encrypted.

[0007] While it would presumably be possible to simply store the datastream as it is received from the broadcaster for later replay, this technique has distinct disadvantages. One such disadvantage is that it would provide pirates a permanently recorded version of the encrypted datastream, thus providing the pirate with information that can be used to perform detailed analyses of the datastream itself to determine the encryption techniques and codes.

[0008] What is needed is a system and method for se-

SDOCID: <EP___1176826A2_I_>

curely recording broadcast media programs (including impulse purchase pay-per-view programs) for limited use playback at a later time. Such a system could be used to support video-on-demand (VOD), thus allowing the subscriber to purchase media programs and games from the set top box instantly without worrying about the start time of the program. What is also needed is a system and method that does not require substantial changes to subscriber hardware, such as the integrated receiver/decoder (IRD), or the conditional access module (CAM) that is used to provide a key to decrypt the media programs for presentation to the subscribers.

SUMMARY OF THE INVENTION

[0009] In summary, the present invention describes a system and method for storing and retrieving program material for subsequent replay. The method comprises the steps of receiving a data stream comprising the program material encrypted according to a first encryption key and control data, the control data comprising the first encryption key and being encrypted; further encrypting the encrypted program material according to a second encryption key; encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; storing the further encrypted program material and control data and the fourth encryption key.

[0010] The apparatus comprises a tuner, for receiving a data stream comprising encrypted access control information and the program material encrypted according to a first encryption key, the access control information including the first encryption key; a first encryption module, communicatively coupled to the tuner and communicatively coupleable to a media storage device, for further encrypting the encrypted program material according to a second encryption key and for encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; a first decryption module communicatively coupleable to the media storage device, for decrypting the fourth encryption key retrieved from the media storage device using the third encryption key to produce the second encryption key, and for decrypting the further encrypted program material retrieved from the media program device to produce the encrypted program material; a conditional access module communicatively coupled to the first decryption module, for decrypting the encrypted access control information to produce the first encryption key; and a second decryption module, for decrypting the program material using the first encryption key.

[0011] One object of the present invention is to provide a system allowing for growth to pay-per-play or true video-on-demand (VOD) services from media programs stored on a hard disk. The pay-per-play service allows the subscriber to select media programs or games from the real time broadcast data or from the media programs stored on the disk. VOD service permits the subscriber to purchase provided media programs and games from the subscriber's receiver instantly, without regard to the start time of the program.

[0012] Another object of the present invention is to provide for the reception and decryption of broadcast media programs, including impulse pay-per-view (IPPV) programs, that can be played and recorded onto storage media and allows playback at a later time with limited use. The data itself may be placed in short term storage, but the replay of the media programs can be accomplished with trick play functions such as forward, reverse, fast forward, fast reverse, frame advance, and pause functions.

[0013] Another object of the present invention is to provide PVR functions which provide recording, delayed playback, and trick play of IPPV media programs from the storage media without requiring a pre-purchase of the IPPV media program. This would allow the IPPV media program to be viewed without requiring the IPPV media program to be purchased prior to storage. Ideally, such a system would allow the user to select the IPPV media program from the storage device, subject to limited play rights.

[0014] Still another object of the present invention is to provide a pairing between the storage media and elements of the subscriber's IRD to assure that playback of the media programs from the storage device are permitted only with the proper IRD.

[0015] Still another object of the present invention is to provide a secure means for storing broadcast data streams (including IPPV and games) on a data storage device, while providing for adequate copy protection.

[0016] Still another object of the present invention is to provide a system and method for handling the archiving and retrieving of media programs and other data, even if the data storage device fails.

[0017] Still another object of the present invention is to provide a system and method that allows media program purchases to be recorded in a way that is analogous to that which is employed for real-time off-the-air programs.

[0018] Still another object of the present invention is to provide a system that provides a growth path to a system permitting IPPV media programs to be previewed without charge for an initial period of time with the option to purchase the media program or cancel the purchase, regardless of whether the program is retrieved from the storage device or obtained from a real time broadcast.

[0019] The present invention eliminates concerns regarding the proliferation of unauthorized digital copies of the media programs by use of a strong encryption method. Further, the present invention ensures that the stored material cannot be distributed since such decryption of the material can only be successfully performed by the encrypting IRD. At the same time, the present invention can be implemented with minimal changes to the IRD, and no changes to the CAM interface. The present invention also provides a basis for a growth path to more advanced encryption/decryption techniques.

DOCID: <EP___1176826A2_I_>

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] Referring now to the drawings in which like reference numbers represent corresponding parts throughout:

FIG. 1 is a diagram showing an overview of a video distribution system;
FIG. 2 is a block diagram showing a typical uplink configuration showing how video program material is uplinked to a satellite for transmission to subscribers using a single transponder;
FIG. 3A is a diagram of a representative data stream received from a satellite;
FIG. 3B is a diagram illustrating the structure of a data packet;
FIG. 4 is a block diagram illustrating a high-level block diagram of the IRD;
FIG. 5 is a diagram illustrating the storage and retrieval of data from a media storage device; and
FIG. 6 is a diagram illustrating the storage and retrieval of data from the media storage device in an alternative embodiment of the invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0021] In the following description, reference is made to the accompanying drawings which form a part hereof, and which show, by way of illustration, several embodiments of the present invention. It is understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

VIDEO DISTRIBUTION SYSTEM

[0022] FIG. 1 is a diagram illustrating an overview of a video distribution system 100. The video distribution system 100 comprises a control center 102 in communication with an uplink center 104 via a ground or other link 114 and an integrated receiver/decoder (IRD) 132 at receiver station 130 via a public switched telephone network (PSTN) or other link 120. The control center 102 provides program material to the uplink center 104, coordinates with the receiver station 130 to offer subscribers 110 pay-per-view (PPV) program services, including billing and associated decryption of video programs.

[0023] The uplink center 104 receives program material and program control information from the control center 102, and using an uplink antenna 106, transmits the program material and program control information to the satellite 108. The satellite 108 receives and processes this information, and transmits the video programs and control information to the IRD 132 at the receiver station 130 via downlink 118. The IRD 132 receives this information using the subscriber antenna 112 to which it is communicatively coupled.

[0024] The video distribution system 100 can comprise a plurality of satellites 108 in order to provide wider terrestrial coverage, to provide additional channels, or to provide additional bandwidth per channel. In one embodiment of the invention, each satellite comprises 16 transponders to receive and transmit program material and other control data from the uplink center 104 and provide it to the subscribers 110. However, using data compression and multiplexing techniques the channel capabilities are far greater. For example, two-satellites 108 working together can receive and broadcast over 150 conventional (non-HDTV) audio and video channels via 32 transponders.

[0025] While the invention disclosed herein will be described with reference to a satellite based video distribution system 100, the present invention may also be practiced with terrestrial-based transmission of program information, whether by traditional broadcasting means, cable, or other means. Further, the different functions collectively allocated among the control center 102 and the uplink center 104 as described above can be reallocated as desired without departing from the intended scope of the present invention.

[0026] Although the foregoing has been described with respect to an embodiment in which the program material delivered to the subscriber is video (and audio) program material such as a movie, the foregoing method can be used to deliver program material comprising purely audio information or data as well.

[0027] FIG. 2 is a block diagram showing a typical uplink configuration for a single satellite 108 transponder, showing how video program material is uplinked to the satellite 108 by the control center 102 and the uplink center 104. FIG. 2 shows three video channels (which could be augmented respectively with one or more audio channels for high fidelity music, soundtrack information, or a secondary audio program for transmitting foreign languages), and a data channel from a computer data source 206.

[0028] The video channels are provided by a program source of video material 200A-200C (collectively referred to hereinafter as video source(s) 200). The data from each video program source 200 is provided to an encoder 202A-202C (collectively referred to hereinafter as encoder(s) 202). Each of the encoders accepts a presentation time stamp (PTS) from the controller 216. The PTS is a wrap-around binary time stamp that is used to assure that the video information is properly synchronized with the audio information after encoding and decoding. A PTS time stamp is sent with each I-frame of the MPEG encoded data.

[0029] In one embodiment of the present invention, each encoder 202 is a second generation Motion Picture Experts Group (MPEG-2) encoder, but other decoders implementing other coding techniques can be used as well. The data channel can be subjected to a similar compression scheme by an encoder (not shown), but such compression is usually either unnecessary, or per-

SDOCID: <EP__1176826A2_I_>

formed by computer programs in the computer data source (for example, photographic data is typically compressed into *.TIF files or *.JPG files before transmission). After encoding by the encoders 202, the signals are converted into data packets by a packetizer 204A-204F (collectively referred to hereinafter as packetizer (s) 204) associated with each source 200, 206-210.

[0030] The data packets are assembled using a reference from the system clock 214 (SCR), a control word (CW) generated by the conditional access manager 208, and a system channel identifier (SCID) generator 210 that associates each of the data packets that are broadcast to the subscriber with a program channel. This information is transmitted to the packetizers 204 for use in generating the data packets. These data packets are then multiplexed into serial data, encoded, modulated, and transmitted. A special packet known as a control word packet (CWP) which comprises control data including the control word (CW) and other control data used in support of providing conditional access to the program material is also encrypted and transmitted.

[0031] FIG. 3A is a diagram of a representative data stream. The first packet segment 302 comprises information from video channel 1 (data coming from, for example, the first video program source 200A). The next packet segment 304 comprises computer data information that was obtained, for example from the computer data source 206. The next packet segment 306 comprises information from video channel 5 (from one of the video program sources 200), and the next packet segment includes information from video channel 1 (again, coming from the first video program source 200A). The data stream therefore comprises a series of packets from any one of the data sources in an order determined by the controller 216. The data stream is encrypted by the encryption module 218, modulated by the modulator 220 (typically using a QPSK modulation scheme), and provided to the transmitter 222, which broadcasts the modulated data stream on a frequency bandwidth to the satellite via the antenna 106.

[0032] Subscribers 110 receive media programs via a subscriber receiver or IRD 132. Using the SCID, the IRD 132 reassembles the packets to regenerate the program material for each of the channels. As shown in FIG. 3A, null packets created by the null packet module 312 may be inserted into the data stream as desired.

[0033] FIG. 3B is a diagram of a data packet. Each data packet (e.g. 302-316) is 147 bytes long, and comprises a number of packet segments. The first packet segment 320 comprises two bytes of information containing the SCID and flags. The SCID is a unique 12-bit number that uniquely identifies the data packet's data channel. The flags include 4 bits that are used to control whether the packet is encrypted, and what key must be used to decrypt the packet. The second packet segment 322 is made up of a 4-bit packet type indicator and a 4-bit continuity counter. The packet type identifies the packet as one of the four data types (video, audio, data, or null). When combined with the SCID, the packet type determines how the data packet will be used. The continuity counter increments once for each packet type and SCID. The next packet segment 324 comprises 127 bytes of payload data, which is a portion of the video program provided by the video program source 200. The final packet segment 326 is data required to perform forward error correction.

ENCRYPTION OF MEDIA PROGRAMS

[0034] Media programs are encrypted by the encryption module 218 before transmission to assure that they are received and viewed only by authorized subscribers. Each media program is encrypted according to an alphanumeric encryption key referred to hereinafter as a control word (CW). This can be accomplished by a variety of data encryption techniques, including the data encryption standard (DES) and the Rivest-Shamir-Adleman (RSA) algorithm.

[0035] To decrypt the media programs, the subscriber's 110 IRD 132 must also have access to the CW. To maintain security, CWs are not transmitted to the IRD 132 plaintext. Instead, CWs are encrypted before transmission to the subscriber's IRD 132. The encrypted CW is transmitted to the subscriber's IRD 132 in a control word (data) packet.

[0036] In one embodiment, the data in the CWP, including the CW, is encrypted and decrypted via what is referred to hereinafter as an input/output (I/O) indecipherable algorithm.

[0037] An I/O indecipherable algorithm is an algorithm that is applied to an input data stream to produce an output data stream. Although the input data stream uniquely determines the output data stream, the algorithm selected is such that it's characteristics cannot be deciphered from a comparison of even a large number of input and output data streams. The security of this algorithm can be further increased by adding additional functional elements which are non-stationary (that is, they change as a function of time). When such an algorithm is provided with identical input streams, the output stream provided at a given point in time may be different than the output stream provided at another time.

[0038] So long as the encryption module 218 and the IRD 132 share the same I/O indecipherable algorithm, the IRD 132 can decode the information in the CWP to retrieve the CW. Then, using the CW, the IRD 132 can decrypt the media program so that it can be presented to the subscriber 110.

[0039] To further discourage piracy, the control data needed to decrypt and assemble data packets into viewable media programs may be time-varying (the validity of the control data in a CWP to decode a particular media program changes with time). This can be implemented in a variety of ways.

[0040] For example, since each CWP is associated with a SCID for each media program, the SCID related

DOCID: <EP___1176826A2_I_>

to each CWP could change over time.

[0041] Another way to implement time-varying control data is to associate time stamps with the received data stream and the CWP control data. In this case, successful decoding of the CWP to produce the CW would require the proper relationship between the time stamps for the data stream and the control data in the CWP. This relationship can be defined, for example, by changing the decryption scheme used to generate the CW from the CWP according to the received time stamp for the data stream. In this case, if the time stamp of the received data stream does not match the expected value, the wrong decryption scheme will be selected and the proper CW (to decrypt the program material) will not be produced. If, however, the time stamp of the received data stream matches the expected value, the proper decryption scheme will be selected, and the CWP decryption scheme will yield the proper CW.

REQUESTING PAY-PER-VIEW SERVICES

[0042] The data required to receive pay-per-view (PPV) media programs are stored in the CWP and in another data packet known as the purchase information parcel (PIP). Both the CWP and the PIP are broadcast to the subscriber via the video distribution system 100 in real time. As described below, the CWP is used by the IRD 132 to retrieve PPV media programs.

[0043] Generally, PPV services can include operator-assisted pay-per-view (OPPV) and impulse pay-per-view (IPPV) services. When requesting OPPV services, the subscriber 110 must decide in advance that they desire access to a particular media program. The subscriber 110 then calls an entity such as the control center 102, and requests access to the media program. When requesting impulse pay-per-view services (IPPV), the subscriber 110, while viewing the program guide, moves the cursor over the viewer channel associated with the desired media program, and selects "enter." After the decision and rights to purchase a PPV program are confirmed (for example, by checking channel lockouts, rating limits, and purchase limits), a purchase information parcel (PIP) is received and stored in the subscriber's conditional access module 406 (which is described in more detail below) for further use. The conditional access module 406 associates the information in the CWP and the PIP, and uses the PIP in conjunction with the CWP to verify that the subscriber 110 should be provided access to the media program and to decrypt the media program.

[0044] Ordering PPV media programs in advance using the PIP is limited, however, since the PIP is broadcast up to 24 hours before the media program itself is broadcast. Since the PIP is broadcast in real time, the IRD 132 does not acquire the PIP until the subscriber 110 actually requests the PPV media program purchase.

SUBSCRIBER RECEPTION AND DECRYPTION OF MEDIA PROGRAMS

[0045] FIG. 4 is a simplified block diagram of an IRD 132. The IRD 132 receives and decrypts the media programs broadcast by the video distribution system 100. These media programs are streamed to the IRD 132 in real time, and may include, for example, video, audio, or data services.

[0046] The IRD 132 is communicatively coupleable to a conditional access module (CAM) 406. The CAM 406 is typically implemented in a smart card or similar device, which is provided to the subscriber 110 to be inserted into the IRD 132. The CAM 406 interfaces with a conditional access verifier (CAV) 408 which performs at least some of the functions necessary to verify that the subscriber 110 is entitled to access the media programs. The CAV 408 is communicatively coupled to a metadata analysis module (MAM) 411. Using the information in metadata table (e.g. Table 1 described below), the MAM 411 acts as a gate-keeper to determine whether stored media programs will be decrypted and presented to the subscriber 110. This is accomplished by comparing the metadata values with measured or accumulated values. The CAV 408 and the MAM 411 can be implemented as separate modules from the transport/demux/decryptor 412 and the microcontroller and memory 414 as shown, or may be implemented via software instructions stored in the memory and performed by the microcontroller 414.

[0047] The IRD 132 comprises a tuner 410, a transport and demultiplexing module (TDM) 412, which operates under control of a microcontroller and associated memory 414, a source decoder 416 and communicatively coupled random access memory (RAM) 418, and a user I/O device for accepting subscriber 110 commands and for providing output information to the subscriber.

[0048] The tuner receives the data packets from the video distribution system and provides the packets to the TDM 412. Using the SCIDs associated with each media program, the TDM 412 reassembles the data packets according to the channel selected by the subscriber 110, and unencrypts the media programs using the CW key. The TDM 412 can be implemented by a single secure chip, and is communicatively coupled to a microcontroller and memory 414.

[0049] Once the media programs are unencrypted, they are provided to the source decoder 416 which decodes the media program data according to MPEG or JPEG standards as appropriate. The decoded media program is then provided to a D/A converter (if necessary) and provided to external interfaces 404 which can include a media program presentation device such as a television, an audio system, or a computer. The source decoder 416 makes use of communicatively coupled RAM 418 to perform these functions.

[0050] The CW key is obtained from the CWP using

SDOCID: <EP___1176826A2_I_>

the CAV 408 and the CAM 406. The TDM 412 provides the CWP to the CAM 406 via the CAV 408. The CAM 406 uses the I/O indecipherable algorithm to generate the CW, which is provided back to the TDM 412. The TDM 412 uses the CW to decrypt the media programs. In most IRDs 132, the CAV 408 and the CAM 406 are capable of decrypting one video/audio/data media program at a time.

[0051] As described above, to discourage potential pirates, the control data in the CWP used to decode a particular media program may change with time so that it only produces the proper CW when applied to a media program having the proper time stamp. In this case, the CAM 406 can select and/or control the decryption scheme (e.g. the I/O indecipherable algorithm) according to the time stamp associated with the data stream carrying the media program. If the media program is sufficiently disassociated in time, the improper decryption scheme will be used, and the proper CW to decode the media program will not be produced.

[0052] Further details regarding the encryption and decryption of media programs can be found in co-pending and commonly assigned U.S. Patent Application Serial No. 09/491,959.

STORAGE AND RETRIEVAL OF MEDIA PROGRAMS IN ENCRYPTED FORM

[0053] FIG. 5 is a diagram presenting exemplary method steps used to practice one embodiment of the present invention. A data stream is provided by subscriber antenna 112 and received by the tuner 410 and the TDM 412, as shown in block 502. The data stream includes a plurality of data packets including data packets with the program material 504 encrypted according to a first encryption key (CW key 538) and access control information which is manifested within one or more control word packets (CWP 506). The control word packets 506 include an encrypted version of the CW key 538. The data stream may also include metadata having replay rights. The replay rights are parameters necessary for controlling the replay of IPPV or pay-per-play services.

[0054] The encrypted program material 504 (denoted Encrypted V/A/D in FIG. 5 to indicate that the program material can include video, audio, or other data) is then provided to a first encryption module 552. The first encryption module 552 includes a storage encryption module 508 and a key encryption module (KEM) 516. The CP encryption module 508 encrypts the encrypted program material 504 (thus further encrypting the encrypted program material 504) and the CWP 506 with a copy protection (CP) key 514. In one embodiment, this is accomplished via a triple 56 bit Data Encryption Standard (DES) cipher block chaining (CBC). RSA encryption may also be used, but triple DES is temporally more efficient, and is therefore preferred.

[0055] In one embodiment, the CP key 514 is derived using a CP generation module 546 from the properties of the replay rights and other metadata in the broadcast stream. Depending on the metadata, the CP key 514 may also be time variant with the broadcast program material. In another embodiment, the CP key may be augmented with at least a portion of the metadata before being encrypted with the box key 518 in the KEM 516 and stored in the media storage device as the encrypted CP key 520. In this embodiment, when the encrypted CP key 520 is decrypted, the CP key and related metadata are both produced. The metadata can then be used to verify and/or control replay of the program material. The CP key 514 may also be internally generated by the IRD 132 without the metadata.

[0056] The key encryption module 516 also encrypts the CP key 514 with the box key 518 to produce an encrypted CP key 520. In one embodiment, the box key 518 is stored within the IRD 132. For example, the box key 518 could be an internal electronic serial number (ESN) of an integrated circuit implementing some or all of the functions of the TDM 412 (hereinafter, the "transport chip"). Incorporating the ESN into the encryption key ensures that only that IRD 132 that stored the encrypted information in the media storage device can successfully decrypt the stream.

[0057] The further encrypted program material 510, the encrypted CWP 512, and the encrypted CP key 520 is then stored 522 in the media storage device 524. The media storage device 524 is typically a hard drive, but may be any device with sufficient capacity and access time to support recording and/or playback operations of the data stored therein.

[0058] When the subscriber 110 decides to play back the stored media programs, an appropriate user input is provided on the user I/O device 420. The user input may comprise a play command, a fast forward command, a reverse command, a fast play or fast reverse play command, or a pause command. In response to the user input, the stored data is retrieved from the media storage device 524. This data includes the further encrypted program material 510, the encrypted CWP 512, and the encrypted CP key 520. The encrypted CP key 520 is decrypted using the box key 518 to produce the CP key 514. This CP key 514 is used to decrypt the further encrypted media program material 510 and the encrypted CWP 512 to produce the encrypted media program 504 and the CWP 506, respectively. The CWP 506 is provided to the CAM 406.

[0059] The IPPV control module 532 determines whether the requested media program is a PPV program (IPPV or OPPV). If so, the subscriber 110 is informed that the media program selected is a PPV program. If the subscriber 110 elects to receive the PPV program, a PPV request is accepted, and the purchase history module 534 collects and records the information regarding the requested program material so that the subscriber 110 can be billed for viewing the media program. In one embodiment, the PPV request is compared

EDOCID: <EP___1176826A2_I_>

to the replay right information in the metadata to determine if the program material that is the subject of the PPV request should be decrypted and provided. For example, the replay right metadata could be used to indicate that the program could be viewed for a specific period of time, or for a particular number of showings.

[0060] The CWP 506 is then provided to the CW extraction module 536, which produces the CW key 538. In one embodiment, this is accomplished in the CAM 406 via application of the I/O indecipherable algorithm discussed above. Using the CW key 538, the encrypted program material 504 is decrypted to produce a clear version of the media program 542.

[0061] Using the foregoing scheme, the encrypted program material and the CWP 506 must be tracked and correlated during decryption by the IRD 132. This may be accomplished by correlation through time stamps, and/or MPEG I and P frames. Since each playback of program requires the CP decryption (via CP key 538) and the CA decryption (via CW) process, the decryption may be slowed enough to cause video lagging or blank out during trick play functions. This problem could be minimized by setting aside sufficient buffer memory to handle the decoded video.

[0062] After suitable processing (i.e. MPEG and or JPEG decoding, decompression, conversion to an analog signal, etc.), the media program is provided to an external interface 404 device, which may include a presentation device such as a display 544.

[0063] In one embodiment of the present invention, the data stream received in IRD 132 further comprises metadata including data to control replay rights and copy protection. This metadata can be encrypted by the CP encrypt module 552 and stored in the media storage device 524 for later decryption and use when a request to view the media program is received. Alternatively, the metadata can be encrypted and broadcast in the data stream in real time for all PPV-enabled media programs, thus obviating the need for storing the information in the media storage device 524.

[0064] As described above, the relationship between the CWP 506 and the encrypted media program may be time-varying. However, in the nominal case described above, since both the CWP 506 and the encrypted program material 504 associated with the same time stamps are stored, replay of the stored material can be performed without modification to either the time stamps or the CWP 506. However, if temporally-limited replay rights are desired, the time stamps or associated with the CWP 506 or the CWP 506 itself may be modified prior to storage.

[0065] Although the foregoing has been described with respect to a plurality of encryption modules (e.g. modules 508 and 516) and decryption modules (e.g. modules 528 and 530), the present invention can be implemented with single encryption module, a single decryption module, or a single encryption/decryption module. In one embodiment of the present invention, the operations performed by modules 508, 516, 528, and 530, are performed in a single integrated circuit device such as the transport chip.

[0066] FIG. 6 is diagram presenting an alternative embodiment of the present invention in which the CWP 506 is stored in the media storage device without encryption by the CP key 514. In this embodiment, the CWP 506 is read from the media storage device 524 and provided to the CAM 406, and need not be decrypted using the CP key 514. One advantage of this embodiment is that it requires fewer encryption and decryption operations, thus allowing the program materials to be more quickly stored and retrieved from the media storage device and presented to the user. This embodiment is particularly advantageous for embodiments using trick play features.

Conclusion

[0067] The present invention describes encryption and decryption functions that enhance the security of the data stored on the disk drive by further encrypting (with a CP or copy protection key) the already encrypted program material comprising a video/audio/data MPEG stream before storage. These encryption and decryption functions are provided by IRD 132, preferably within the transport chip. Since the broadcast data stream is not decrypted before storage on the media storage device, but rather further encrypted, a clear version is not exposed to possible compromise before storage on the media storage device. Further, since the encrypted broadcast stream is further encrypted before storage, the encrypted broadcast stream is not available for potential pirates to analyze to try to break the broadcast stream encryption scheme.

[0068] In one embodiment, metadata is included in the data stream broadcast to the IRD 132. This metadata includes replay rights and other parameters necessary for controlling the replay of the media program. This replay rights included in this metadata and/or the broadcast time of the program material can be used to derive the CP key 514 that is used to further encrypt (already) encrypted program material.

[0069] The program material requested for storage into the media storage device includes the further encrypted version of the encrypted program material and the CWP 506. This further encrypted data is not decrypted until the user starts the playback of the program from the media storage device.

[0070] Once playback is initiated, the further encrypted data and the encrypted CWP 506 is decrypted using the CP key 514. The decrypted CWP 506 is provided to the CAM 406. The CAM 406 decrypts the CWP 506, and provides the resulting CW 538 to a broadcast decryption module to decrypt the encrypted program material.

[0071] The present invention protects the data stored in the media storage device from pirates and does not expose the program material in an unencrypted form un-

SDOCID: <EP__1176826A2_I_>

til the viewer has requested (and paid for) the program material. Further, this is accomplished without introducing additional CAM 406 functions. By using the metadata to derive a CP key 514 to scramble the encrypted program data and CAM 406, the present invention provides additional security, while providing a growth path permit more advanced pay per view features The foregoing description of the preferred embodiment of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. For example, the encryption functions described herein could be performed by separate encryption/decryption modules, or a single multi-purpose encryption/decryption module can be utilized to perform the encryption/decryption functions of many separate modules.

[0072] The foregoing description of the preferred embodiment of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. It is intended that the scope of the invention be limited not by this detailed description, but rather by the claims appended hereto. The above specification, examples and data provide a complete description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

Claims

1. A method of storing program material for subsequent replay, comprising the steps of:

   receiving a data stream comprising the program material encrypted according to a first (CW) encryption key and control data, the control data comprising the first (CW) encryption key and being encrypted;
   further encrypting the encrypted program material (504) according to a second encryption key (514);
   encrypting the second encryption key (514) according to a third encryption key (518) to produce a fourth encryption key (520); and
   storing the further encrypted program material (510) and control data and the fourth encryption key (520).

2. The method of claim 1, further comprising the steps of:

   retrieving the stored further encrypted program material (510), control data and the fourth encryption key (520);
   decrypting the fourth encryption key (520) using the third encryption key (518) to produce the second encryption key (514);
   decrypting the further encrypted program material (510) with the second encryption key (514) to produce the encrypted program material (504);
   decrypting the control data to produce the first (CW) encryption key; and
   decrypting the encrypted program material (504) using the first (CW) encryption key.

3. The method of claim 2, further comprising the steps of:

   accepting a PPV request before decrypting the encrypted program material using the first (CW) encryption key; and
   recording billing information regarding the program material.

4. The method of claim 2, further comprising the steps of:

   further encrypting the control data according to the second encryption key (514);
   storing the further encrypted control data (512); and
   decrypting the further encrypted control data (512) according to the second encryption key (514).

5. The method of claim 1, wherein the data stream further comprises metadata describing program material replay rights.

6. The method of claim 5, wherein the second encryption key (514) is derived at least partially from the metadata.

7. The method of claim 6, wherein the second encryption key (514) is derived at least partially from the broadcast time of the program material.

8. The method of claim 7, further comprising the step of augmenting the second encryption key (514) with at least a portion of the metadata before encrypting the second encryption key (514) according to the third encryption key (518).

9. The method of claim 8, further comprising the steps of:

   retrieving the stored further encrypted program material (510), control data and the fourth encryption key (520);

:DOCID: <EP___1176826A2_I_>

decrypting the fourth encryption key (520) using the third encryption key (518) to produce the second encryption key (514) and the portion of the metadata;

decrypting the further encrypted program material (510) with the second encryption key (514) to produce the encrypted program material (504);

accepting a PPV request; and

determining if the PPV request is permitted using the portion of the metadata; and

decrypting the control data to produce the first (CW) encryption key and decrypting the encrypted program material using the first (CW) encryption key if the PPV request is permitted.

10. A receiver (132) for storing program material for subsequent replay, comprising:

a tuner (410), for receiving a data stream comprising encrypted access control information and the program material encrypted according to a first (CW) encryption key, the access control information including the first encryption key;

a first encryption module (552), communicatively coupled to the tuner (410) and communicatively coupleable to a media storage device (524), for further encrypting the encrypted program material according to a second encryption key (514) and for encrypting the second encryption key (514) according to a third encryption key (518) to produce a fourth encryption key (520);

a first decryption module (550) communicatively coupleable to the media storage device (524), for decrypting the fourth encryption key (520) retrieved from the media storage device (524) using the third encryption key (518) to produce the second encryption key (514), and for decrypting the further encrypted program material (510) retrieved from the media program device (524) to produce the encrypted program material (514);

a conditional access module (406) communicatively coupled to the first decryption module (552), for decrypting the encrypted access control information to produce the first (CW) encryption key; and

a second decryption module (540), for decrypting the program material using the first (CW) encryption key.

11. The apparatus of claim 10, wherein:

the first encryption module (552) further encrypts the encrypted access control information according to the second encryption key (514);

and

the first decryption module (550) further decrypts the further encrypted access control information according to the second encryption key (514).

ISDOCID: <EP___1176826A2_I_>

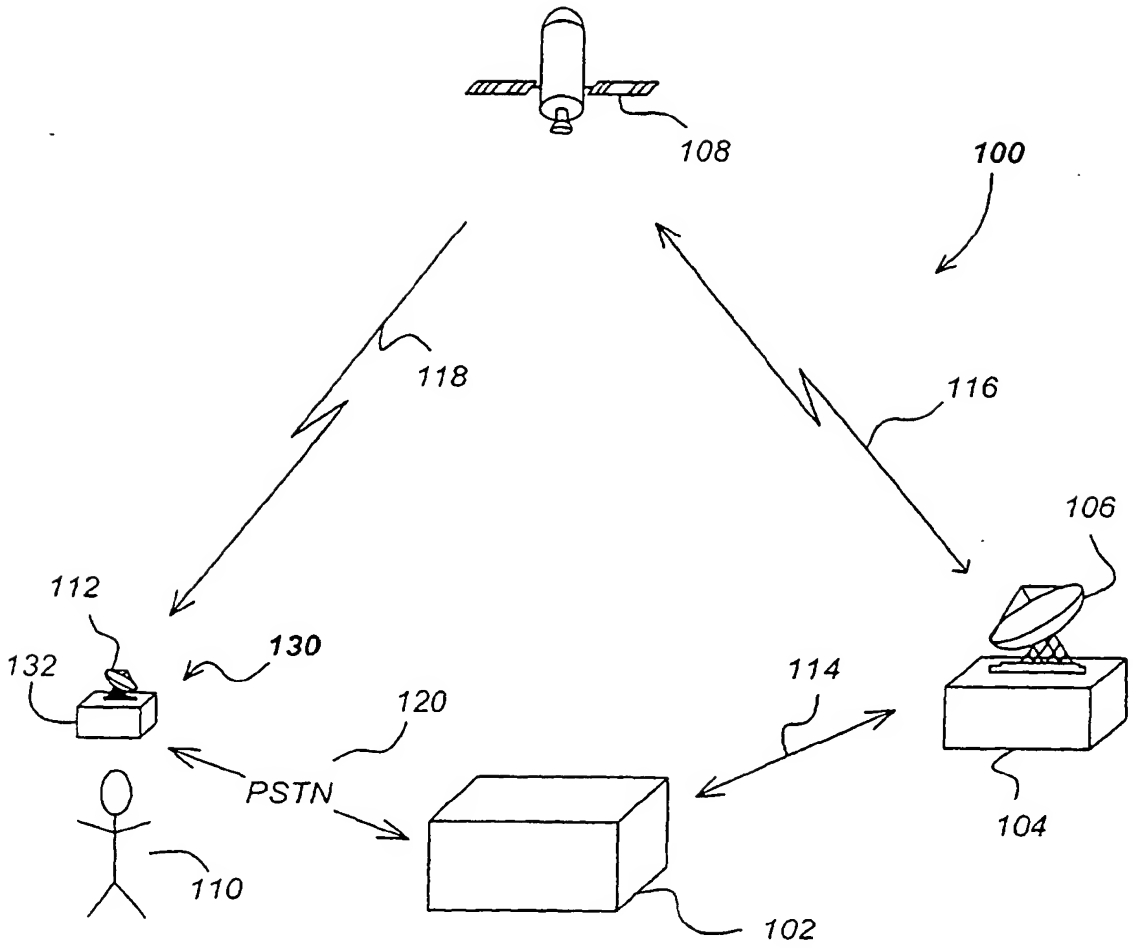

FIG. 1

iDOCID: <EP___1176826A2_I_>

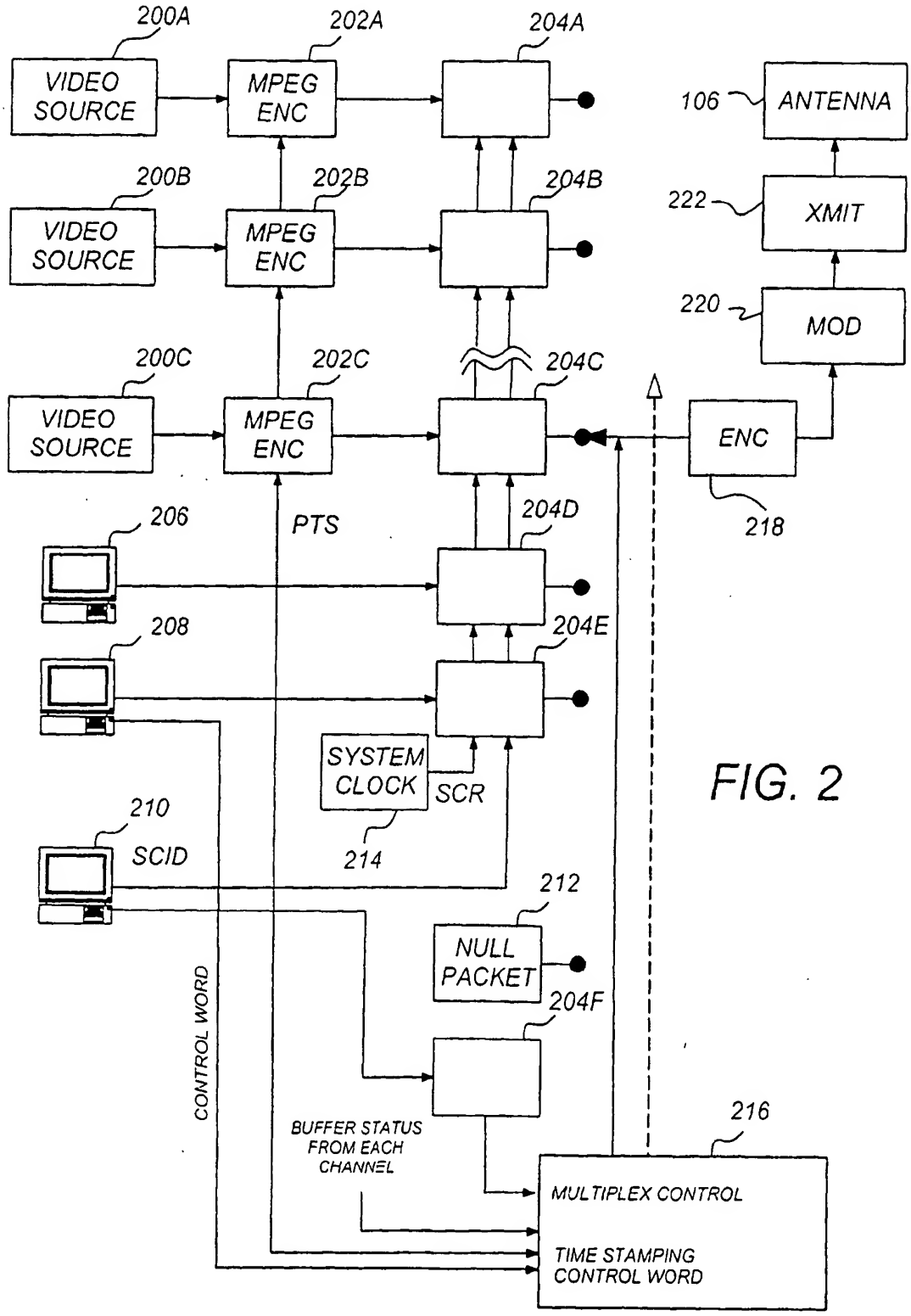

FIG. 2

EDOCID: <EP___1176826A2_I_>

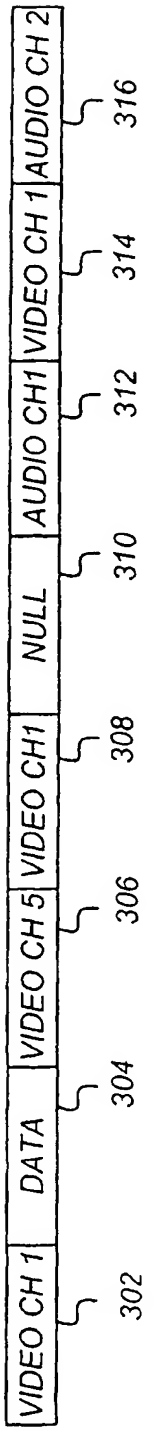

FIG. 3A

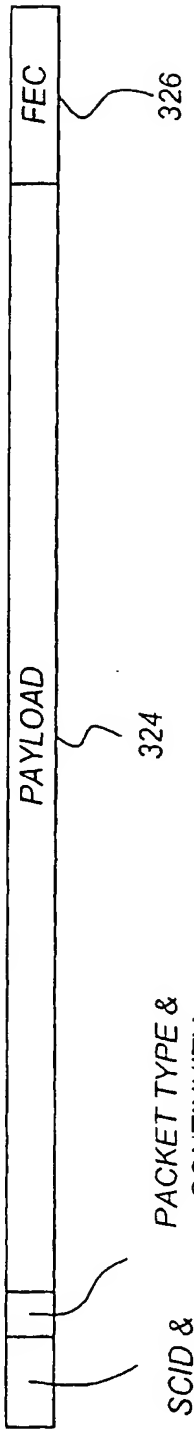

FIG. 3B

DOCID: <EP___1176826A2_I_>

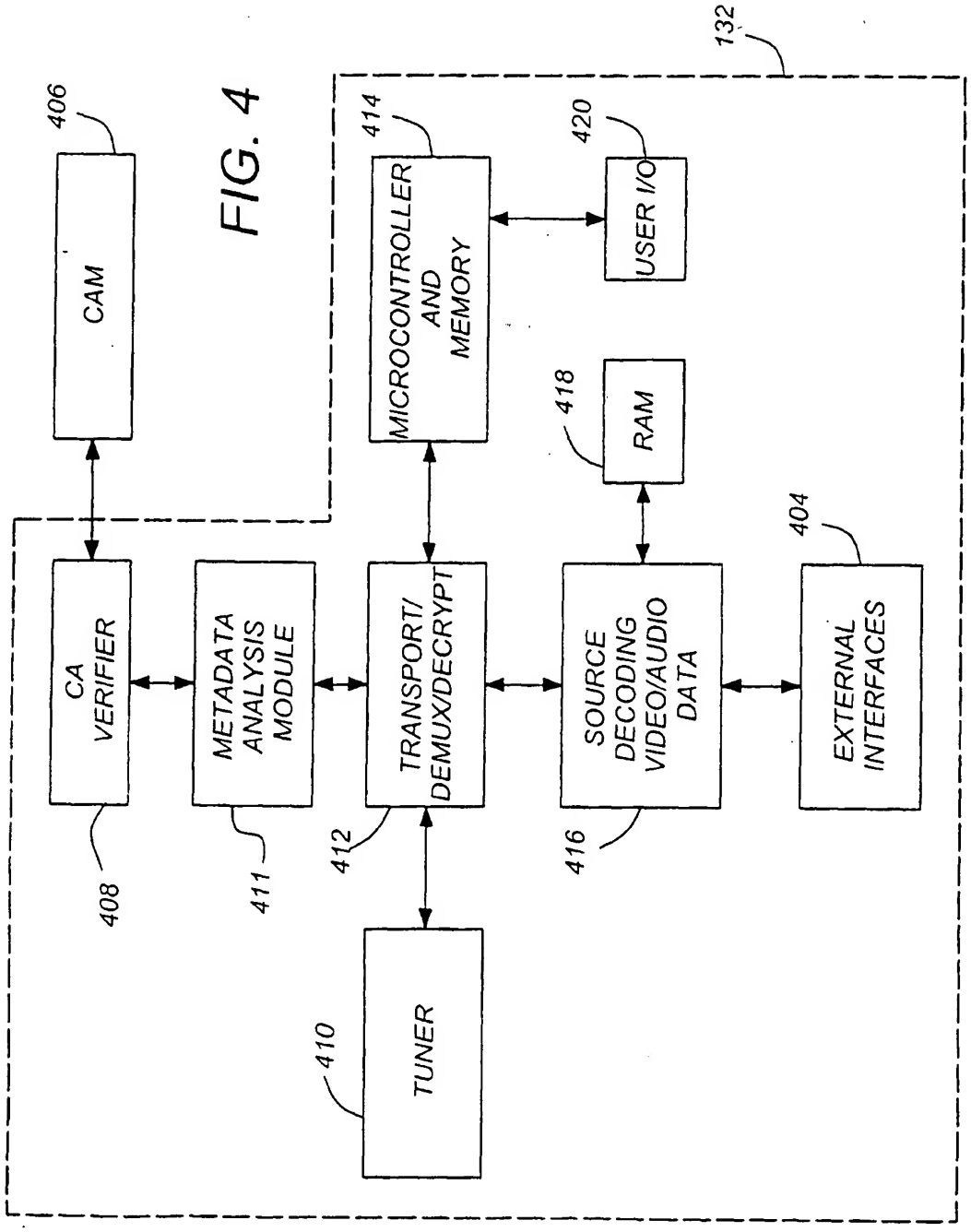

FIG. 4

ISDOCID: <EP___1176826A2_I_>

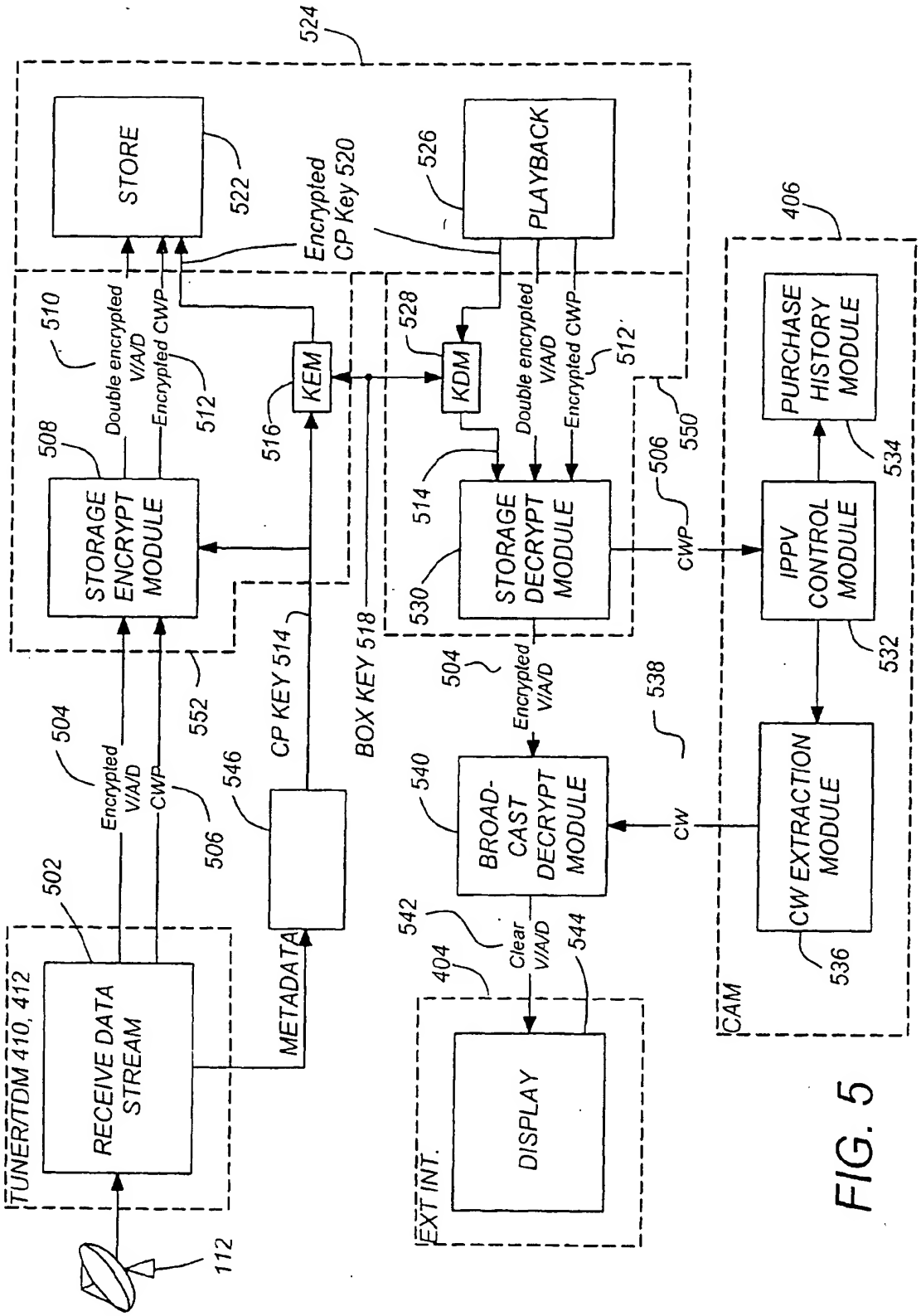

FIG. 5

DOCID: <EP___1176826A2_I_>

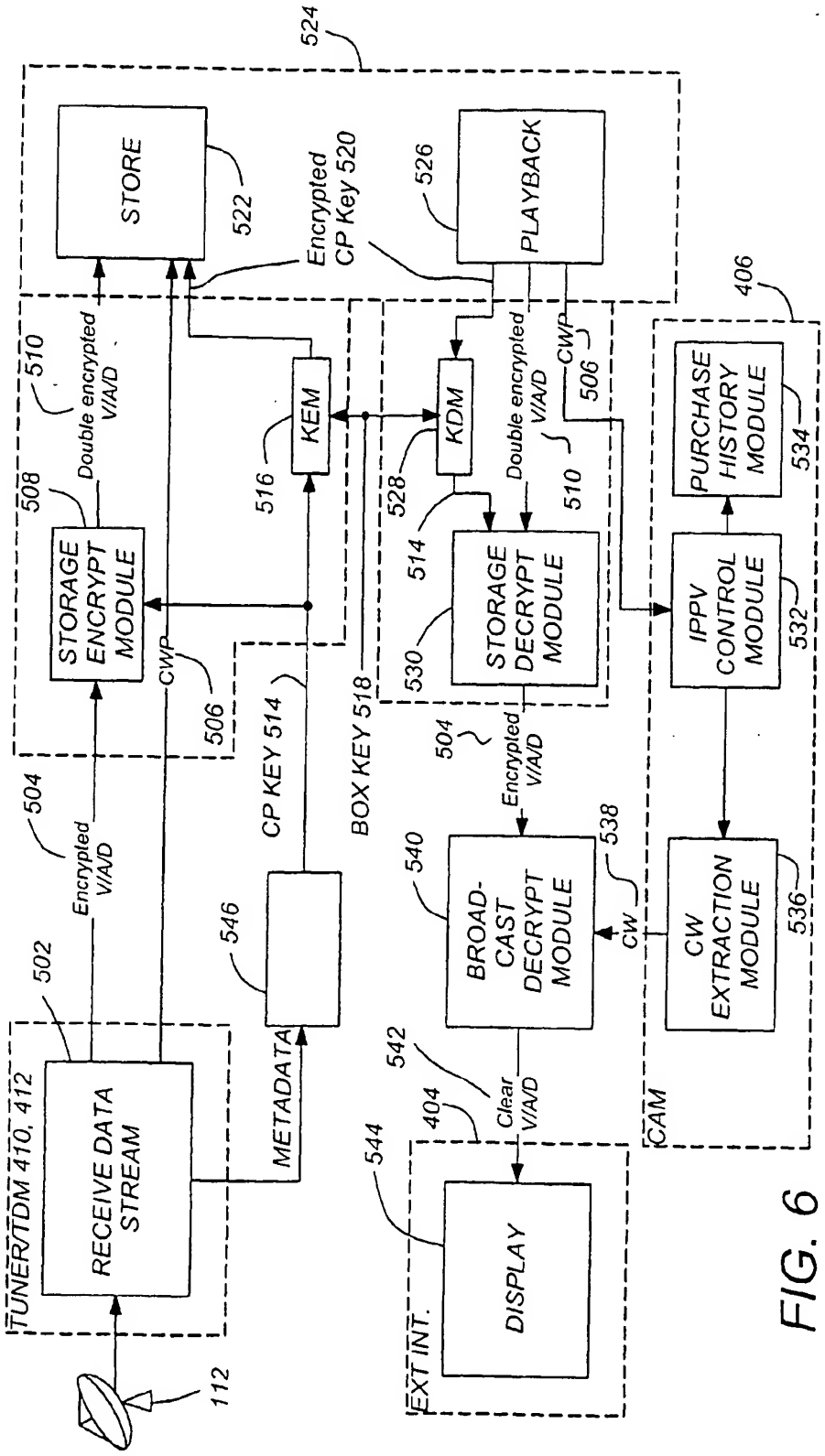

FIG. 6

SDOCID: <EP___1176826A2_I_>

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 176 826 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
30.07.2003 Bulletin 2003/31

(43) Date of publication A2:
30.01.2002 Bulletin 2002/05

(21) Application number: **01117554.4**

(22) Date of filing: **20.07.2001**

(51) Int Cl.[7]: **H04N 7/167**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **21.07.2000 US 621476**

(71) Applicant: **Hughes Electronics Corporation**
El Segundo, California 90245-0956 (US)

(72) Inventors:
- **Kahn, Raynold M.**
  Los Angeles, California 90036 (US)
- **Gagnon, Gregory J.**
  Torrance, California 90277 (US)
- **Ha, David D.**
  San Gabriel, California 91755 (US)
- **Klauss, Peter M.**
  Torrance, California 90503 (US)
- **Curren, Christopher P.**
  Brentwood, California 90049 (US)
- **James, Thomas H.**
  Pacific Palisades, California 90272 (US)

(74) Representative: **Grünecker, Kinkeldey,**
Stockmair & Schwanhäusser Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

(54) Super encrypted storage and retrieval of media programs in a hard-paired receiver and storage device

(57) A method and apparatus for storing and retrieving program material for subsequent replay is disclosed. The apparatus comprises a tuner (410), for receiving a data stream comprising encrypted access control information and the program material encrypted according to a first (CW) encryption key, the access control information including the first encryption key; a first encryption module (552), communicatively coupled to the tuner (410) and communicatively coupleable to a media storage device (524), for further encrypting the encrypted program material according to a second encryption key (514) and for encrypting the second encryption key (514) according to a third encryption key (518) to produce a fourth encryption key (520); a first decryption module (550) communicatively coupleable to the media storage device (524), for decrypting the fourth encryption key (520) retrieved from the media storage device (524) using the third encryption key (518) to produce the second encryption key (514), and for decrypting the further encrypted program material (510) retrieved from the media program device (524) to produce the encrypted program material (514); a conditional access module (406) communicatively coupled to the first decryption module (552), for decrypting the encrypted access control information to produce the first (CW) encryption key; and a second decryption module (540), for decrypting the program material using the first (CW) encryption key.

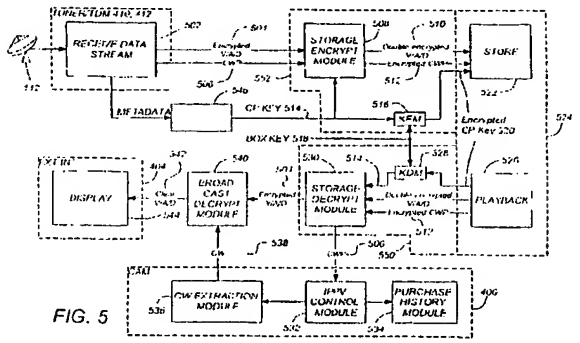

FIG. 5

EP 1 176 826 A3

DOCID: <EP___1176826A3_I_>

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 11 7554

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y	US 5 912 969 A (OKAMOTO HIROO ET AL) 15 June 1999 (1999-06-15) * column 4, line 1 - line 18 * * column 5, line 3 - line 26 * * column 6, line 57 - column 7, line 40; figures 2,3,11 * ---	1-6,10, 11	H04N7/167
Y	EP 0 989 557 A (MATSUSHITA ELECTRIC IND CO LTD) 29 March 2000 (2000-03-29) * column 7, line 22 - column 10, line 22; figures 1-4 * ---	1-6,10, 11	
Y	"1ST REPORT OF EBU / SMPTE TASK FORCE FOR HARMONIZED STANDARDS FOR THE EXCHANGE OF TELEVISION PROGRAM MATERIAL AS BIT STREAMS" EBU REVIEW- TECHNICAL, EUROPEAN BROADCASTING UNION. BRUSSELS, BE, no. 272, 21 June 1997 (1997-06-21), pages 1-73, XP000720137 ISSN: 0251-0936 * page 14 - page 20 * * page 47 - page 48 * ---	5,6	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04N
A	EP 0 975 165 A (SONY CORP) 26 January 2000 (2000-01-26) * column 4, line 27 - column 5, line 17 * * column 7, line 31 - column 9, line 40; figures 1-3,6,7 * * column 10, line 56 - column 11, line 11 * ---	1-7,9-11	
A	WO 00 13412 A (BEYERS WILLIAM WESLEY JR ;ESKICIOGLU AHMET MURSUIT (US); THOMSON C) 9 March 2000 (2000-03-09) * page 8, line 28 - page 12, line 13; figures 2A-2C * -----	1,2,4,8, 10	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
MUNICH	5 June 2003	GIL ZAMORANO, A

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

SDOCID: <EP___1176826A3_I_>

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 11 7554

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

05-06-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5912969 A	15-06-1999	JP 3139910 B2	05-03-2001
		JP 7272399 A	20-10-1995
EP 0989557 A	29-03-2000	JP 11213552 A	06-08-1999
		JP 11232776 A	27-08-1999
		EP 0989557 A1	29-03-2000
		CN 1262770 T	09-08-2000
		WO 9938164 A1	29-07-1999
EP 0975165 A	26-01-2000	EP 1126705 A2	22-08-2001
		EP 1244306 A2	25-09-2002
		EP 0975165 A2	26-01-2000
		CN 1390044 A	08-01-2003
		CN 1390043 A	08-01-2003
		CN 1390055 A	08-01-2003
		CN 1390056 A	08-01-2003
		CN 1390057 A	08-01-2003
		CN 1390053 A	08-01-2003
		CN 1389994 A	08-01-2003
		CN 1390054 A	08-01-2003
		CN 1115150 A ,B	17-01-1996
		DE 69523220 D1	22-11-2001
		DE 69523220 T2	13-06-2002
		DE 69530622 D1	05-06-2003
		EP 0691787 A1	10-01-1996
		JP 8077706 A	22-03-1996
		JP 2003134104 A	09-05-2003
		JP 2003101942 A	04-04-2003
		JP 2003116120 A	18-04-2003
		JP 2003116101 A	18-04-2003
		US 5796828 A	18-08-1998
		US RE38007 E1	25-02-2003
WO 0013412 A	09-03-2000	AU 756954 B2	30-01-2003
		AU 6383799 A	21-03-2000
		BR 9913243 A	22-05-2001
		CN 1332933 T	23-01-2002
		DE 69901618 D1	04-07-2002
		DE 69901618 T2	05-12-2002
		EP 1110393 A1	27-06-2001
		JP 2002525779 T	13-08-2002
		WO 0013412 A1	09-03-2000

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

EDOCID: <EP___1176826A3_I_>

This Page Blank (uspto)